3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.1.A1 Authentisierung (B)

Der IT-Betrieb MUSS Webanwendungen und Webservices so konfigurieren, dass sich Clients gegenüber der Webanwendung oder dem Webservice authentisieren müssen, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür MUSS eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess SOLLTE dokumentiert werden.

Der IT-Betrieb MUSS geeignete Grenzwerte für fehlgeschlagene Anmeldeversuche festlegen.

APP.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A4 Kontrolliertes Einbinden von Dateien und Inhalten (B)

Falls eine Webanwendung oder ein Webservice eine Upload-Funktion für Dateien anbietet, MUSS diese Funktion durch den IT-Betrieb so weit wie möglich eingeschränkt werden. Insbesondere MÜSSEN die erlaubte Dateigröße, erlaubte Dateitypen und erlaubte Speicherorte festgelegt werden. Es MUSS festgelegt werden, welche Clients die Funktion verwenden dürfen. Auch MÜSSEN Zugriffs- und Ausführungsrechte restriktiv gesetzt werden. Zudem MUSS sichergestellt werden, dass Clients Dateien nur im vorgegebenen erlaubten Speicherort speichern können.

APP.3.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A7 Schutz vor unerlaubter automatisierter Nutzung (B)

Der IT-Betrieb MUSS sicherstellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei MUSS jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Clients auswirken. Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, MUSS dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.

APP.3.1.A14 Schutz vertraulicher Daten (B)

Der IT-Betrieb MUSS sicherstellen, dass Zugangsdaten zur Webanwendung oder zum Webservice serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden. Dazu MÜSSEN Salted Hash-Verfahren verwendet werden.

Die Dateien mit den Quelltexten der Webanwendung oder des Webservices MÜSSEN vor unerlaubten Abrufen geschützt werden.

APP.3.1.A16 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A19 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.1.A8 Systemarchitektur (S) [Beschaffungsstelle]

Sicherheitsaspekte SOLLTEN bereits während der Planung von Webanwendungen und Webservices betrachtet werden. Auch SOLLTE darauf geachtet werden, dass die Architektur der Webanwendung oder des Webservice die Geschäftslogik der Institution exakt erfasst und korrekt umsetzt.

APP.3.1.A9 Beschaffung von Webanwendungen und Webservices (S)

Zusätzlich zu den allgemeinen Aspekten der Beschaffung von Software SOLLTE die Institution mindestens folgendes bei der Beschaffung von Webanwendungen und Webservices berücksichtigen:

- sichere Eingabevalidierung und Ausgabekodierung,
- sicheres Session-Management,
- sichere kryptografische Verfahren,
- sichere Authentisierungsverfahren,
- sichere Verfahren zum serverseitigen Speichern von Zugangsdaten,
- geeignetes Berechtigungsmanagement,
- ausreichende Protokollierungsmöglichkeiten,
- regelmäßige Sicherheitsupdates durch den Entwickelnden der Software,
- Schutzmechanismen vor verbreiteten Angriffen auf Webanwendungen und Webservices sowie
- Zugriff auf den Quelltext der Webanwendung oder des Webservices.

APP.3.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A11 Sichere Anbindung von Hintergrundsystemen (S)

Der Zugriff auf Hintergrundsysteme, auf denen Funktionen und Daten ausgelagert werden, SOLLTE ausschließlich über definierte Schnittstellen und von definierten IT-Systemen aus möglich sein. Bei der Kommunikation über Netz- und Standortgrenzen hinweg SOLLTE der Datenverkehr authentisiert und verschlüsselt werden.

APP.3.1.A12 Sichere Konfiguration (S)

Webanwendungen und Webservices SOLLTEN so konfiguriert sein, dass auf ihre Ressourcen und Funktionen ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade zugegriffen werden kann. Der Zugriff auf nicht benötigte Ressourcen und Funktionen SOLLTE deaktiviert werden. Falls dies nicht möglich ist, SOLLTE der Zugriff soweit wie möglich eingeschränkt werden. Folgendes SOLLTE bei der Konfiguration von Webanwendungen und Webservices umgesetzt werden:

- Deaktivieren nicht benötigter HTTP-Methoden,
- Konfigurieren der Zeichenkodierung,
- Vermeiden von sicherheitsrelevanten Informationen in Fehlermeldungen und Antworten,
- Speichern von Konfigurationsdateien außerhalb des Web-Root-Verzeichnisses sowie
- Festlegen von Grenzwerten für Zugriffsversuche.

APP.3.1.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A21 Sichere HTTP-Konfiguration bei Webanwendungen (S)

Zum Schutz vor Clickjacking, Cross-Site-Scripting und anderen Angriffen SOLLTE der IT-Betrieb geeignete HTTP-Response-Header setzen. Dazu SOLLTEN mindestens die folgenden HTTP-Header verwendet werden:

- Content-Security-Policy,
- Strict-Transport-Security,
- Content-Type,
- X-Content-Type-Options sowie
- Cache-Control.

Die verwendeten HTTP-Header SOLLTEN so restriktiv wie möglich sein.

Cookies SOLLTEN grundsätzlich mit den Attributen *secure*, *SameSite* und *httponly* gesetzt werden.

APP.3.1.A22 Penetrationstest und Revision (S)

Webanwendungen und Webservices SOLLTEN regelmäßig auf Sicherheitsprobleme hin überprüft werden. Insbesondere SOLLTEN regelmäßig Revisionen durchgeführt werden. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert, ausreichend geschützt und vertraulich behandelt werden. Abweichungen SOLLTE nachgegangen werden. Die Ergebnisse SOLLTEN dem ISB vorgelegt werden.

APP.3.1.A23 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.1.A20 Einsatz von Web Application Firewalls (H)

Institutionen SOLLTEN Web Application Firewalls (WAF) einsetzen. Die Konfiguration der eingesetzten WAF SOLLTE auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices SOLLTE die Konfiguration der WAF geprüft werden.

APP.3.1.A24 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.3.1.A25 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Open Web Application Security Projekt (OWASP) stellt auf seiner Webseite Hinweise zur Absicherung von Webanwendungen und Webservices zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102" Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.2 Webserver

1. Beschreibung

1.1. Einleitung

Ein Webserver ist die Kernkomponente jedes Webangebotes, er nimmt Anfragen der Clients entgegen und liefert die entsprechenden Inhalte zurück. Die Daten werden in der Regel über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS) transportiert. Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Clients bieten, werden sie auch häufig für interne Informationen und Anwendungen in Institutionsnetzen, wie dem Intranet, eingesetzt.

Webserver sind in der Regel direkt im Internet verfügbar und bieten somit eine exponierte Angriffsfläche. Deswegen müssen sie durch geeignete Schutzmaßnahmen abgesichert werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz des Webservers und der Informationen, die durch den Webserver bereitgestellt oder damit verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein muss auf alle Webserver des Informationsverbunds angewendet werden.

Die Bezeichnung Webserver wird sowohl für die Software verwendet, welche die HTTP-Anfragen beantwortet, als auch für die IT-Systeme, auf denen diese Software ausgeführt wird. In diesem Baustein wird vorrangig die Webserver-Software betrachtet. Sicherheitsaspekte des IT-Systems, auf dem die Webserver-Software installiert ist, werden im Baustein SYS.1.1 *Allgemeiner Server* sowie den jeweiligen betriebssystemspezifischen Bausteinen betrachtet.

Empfehlungen, wie Webserver in die Netzarchitektur zu integrieren und mit Firewalls abzusichern sind, finden sich in den Bausteinen NET.1.1 *Netzarchitektur und -design* bzw. NET.3.2 *Firewall*.

Der Baustein behandelt grundsätzliche Aspekte, die für die Bereitstellung von Webinhalten wichtig sind. Dynamische Inhalte, die durch Webanwendungen bereitgestellt werden, sind nicht Gegenstand des vorliegenden Bausteins. Diese werden im Baustein APP.3.1 *Webanwendungen und Webservices* behandelt. Ebenso werden hier keine Webservices betrachtet.

Webbrowser werden in diesem Baustein nicht betrachtet. Anforderungen dazu sind im Baustein APP.1.2 *Webbrowser* zu finden.

In der Regel werden die Verbindungen zu Webservern verschlüsselt. Der Baustein CON.1 *Kryptokonzept* beschreibt, wie die dazu notwendigen kryptografischen Schlüssel sicher verwaltet werden können.

Werden Webserver nicht selbst betrieben, sondern über einen Hosting-Anbieter bereitgestellt, ist der Baustein OPS.2.3 *Nutzung von Outsourcing* zu beachten.

Oft werden Authentisierungsmechanismen für Webserver verwendet. Ergänzende Anforderungen dazu finden sich im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.2 *Webserver* von besonderer Bedeutung.

2.1. Reputationsverlust

Gelingt es bei einem Angriff mit administrativen Rechten auf einen Webserver zuzugreifen, kann darüber eine manipulierte Webseite ausgeliefert werden (Defacement). So kann die Reputation der Institution geschädigt werden. Ebenso kann die Veröffentlichung falscher Informationen, wie zum Beispiel fehlerhafter Produktbeschreibungen, dazu führen, dass die Reputation der Institution in der Öffentlichkeit leidet. Auch kann die Institution abgemahnt werden, wenn auf ihrer Webseite Inhalte veröffentlicht werden, die gegen gesetzliche Vorschriften verstoßen. Ein Schaden kann auch entstehen, wenn die Webseite nicht verfügbar ist und potenzielle Kunden und Kundinnen deshalb zu Mitbewerbern wechseln.

2.2. Manipulation des Webservers

Bei einem Angriff könnten sich unberechtigte Personen Zugriff auf einen Webserver verschaffen und dessen Dateien manipulieren. Es könnte beispielsweise die Konfiguration der Webserver-Software geändert werden, Schadsoftware verbreitet oder Webinhalte modifiziert werden.

2.3. Denial of Service (DoS)

Durch DoS-Angriffe lässt sich die Verfügbarkeit eines Webangebotes gezielt beeinträchtigen, indem beispielsweise einzelne Accounts durch fehlerhafte Anmeldungen gesperrt werden.

Durch DDoS (Distributed Denial of Service)-Angriffe kann ein Webserver teilweise oder auch ganz ausfallen. Für Clients ist das Webangebot dann nur noch sehr langsam oder gar nicht mehr verfügbar. Für viele Institutionen kann ein solcher Ausfall schnell geschäftskritisch werden, z. B. für Online-Shops.

2.4. Verlust vertraulicher Daten

Viele Webserver verwenden noch veraltete kryptografische Verfahren wie RC4 oder SSL. Eine unzureichende Authentisierung bzw. eine ungeeignete Verschlüsselung kann dazu führen, dass die Kommunikation zwischen den Clients und den Webservern mitgelesen oder manipuliert werden kann. Das gleiche gilt für die Kommunikation zwischen dem Webserver und anderen Servern, wie z. B. Load Balancern.

2.5. Verstoß gegen Gesetze oder Regelungen

Für die Veröffentlichung von Webinhalten gibt es verschiedene regulatorische Anforderungen. Neben den Regelungen der Telemedien- und Datenschutzgesetze, sind auch die Regeln des Urheberrechts zu beachten. Verstöße gegen diese Gesetze können rechtliche Konsequenzen nach sich ziehen.

2.6. Fehlende oder mangelhafte Fehlerbehebung

Treten während des Betriebs eines Webservers Fehler auf, kann sich das z. B. auf dessen Verfügbarkeit auswirken. Auch werden eventuell Inhalte unvollständig dargestellt oder Sicherheitsmechanismen fallen aus. Werden Fehler nicht korrekt behandelt, sind sowohl der Betrieb als auch der Schutz der Funktionen und Daten eines Webservers nicht mehr gewährleistet.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.2 *Webserver* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Compliance-Beauftragte, Zentrale Verwaltung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.2.A1 Sichere Konfiguration eines Webservers (B)

Nachdem der IT-Betrieb einen Webserver installiert hat, MUSS er eine sichere Grundkonfiguration vornehmen. Dazu MUSS er insbesondere den Webserver-Prozess einem Konto mit minimalen Rechten zuweisen. Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Ist dies nicht möglich, SOLLTE jeder Webserver auf einem eigenen physischen oder virtuellen Server ausgeführt werden.

Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden. Nicht benötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden.

APP.3.2.A2 Schutz der Webserver-Dateien (B)

Der IT-Betrieb MUSS alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, so schützen, dass sie nicht unbefugt gelesen und geändert werden können.

Es MUSS sichergestellt werden, dass Webanwendungen nur auf einen definierten Verzeichnisbaum zugreifen können (WWW-Wurzelverzeichnis). Der Webserver MUSS so konfiguriert sein, dass er nur Dateien ausliefert, die sich innerhalb des WWW-Wurzelverzeichnisses befinden.

Der IT-Betrieb MUSS alle nicht benötigten Funktionen, die Verzeichnisse auflisten, deaktivieren. Vertrauliche Daten MÜSSEN vor unberechtigtem Zugriff geschützt werden. Insbesondere MUSS der IT-Betrieb sicherstellen, dass vertrauliche Dateien nicht in öffentlichen Verzeichnissen des Webservers liegen. Der IT-Betrieb MUSS regelmäßig überprüfen, ob vertrauliche Dateien in öffentlichen Verzeichnissen gespeichert wurden.

APP.3.2.A3 Absicherung von Datei-Uploads und -Downloads (B)

Alle mithilfe des Webservers veröffentlichten Dateien MÜSSEN vorher auf Schadprogramme geprüft werden. Es MUSS eine Maximalgröße für Datei-Uploads spezifiziert sein. Für Uploads MUSS genügend Speicherplatz reserviert werden.

APP.3.2.A4 Protokollierung von Ereignissen (B)

Der Webserver MUSS mindestens folgende Ereignisse protokollieren:

- erfolgreiche Zugriffe auf Ressourcen,
- fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Server-Fehlern sowie
- allgemeine Fehlermeldungen.

Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.

APP.3.2.A5 Authentisierung (B)

Wenn sich Clients mit Hilfe von Passwörtern am Webserver authentisieren, MÜSSEN diese kryptografisch gesichert und vor unbefugtem Zugriff geschützt gespeichert werden.

APP.3.2.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote (B) [Fachverantwortliche, Zentrale Verwaltung, Compliance-Beauftragte]

Werden über den Webserver Inhalte für Dritte publiziert oder Dienste angeboten, MÜSSEN dabei die relevanten rechtlichen Rahmenbedingungen beachtet werden. Die Institution MUSS die jeweiligen Telemedien- und Datenschutzgesetze sowie das Urheberrecht einhalten.

APP.3.2.A11 Verschlüsselung über TLS (B)

Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, SOLLTEN diese auf so wenige Fälle wie möglich beschränkt werden.

Wenn eine HTTPS-Verbindung genutzt wird, MÜSSEN alle Inhalte über HTTPS ausgeliefert werden. Sogenannter Mixed Content DARF NICHT verwendet werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.2.A8 Planung des Einsatzes eines Webservers (S)

Es SOLLTE geplant und dokumentiert werden, für welchen Zweck der Webserver eingesetzt und welche Inhalte er bereitstellen soll. In der Dokumentation SOLLTEN auch die Informationen oder Dienstleistungen des Webangebots und die jeweiligen Zielgruppen beschrieben werden. Für den technischen Betrieb und die Webinhalte SOLLTEN geeignete Zuständige festgelegt werden.

APP.3.2.A9 Festlegung einer Sicherheitsrichtlinie für den Webserver (S)

Es SOLLTE eine Sicherheitsrichtlinie erstellt werden, in der die erforderlichen Maßnahmen und Zuständigkeiten benannt sind. Weiterhin SOLLTE geregelt werden, wie Informationen zu aktuellen Sicherheitslücken besorgt werden. Auch SOLLTE geregelt werden, wie Sicherheitsmaßnahmen umgesetzt werden und wie vorgegangen werden soll, wenn Sicherheitsvorfälle eintreten.

APP.3.2.A10 Auswahl eines geeigneten Webhosters (S)

Betreibt die Institution den Webserver nicht selbst, sondern nutzt Angebote externer Unternehmen im Rahmen von Webhosting, SOLLTE die Institution bei der Auswahl eines geeigneten Webhosters auf folgende Punkte achten:

- Es SOLLTE vertraglich geregelt werden, wie die Dienste zu erbringen sind. Dabei SOLLTEN Sicherheitsaspekte innerhalb des Vertrags schriftlich in einem Service Level Agreement (SLA) festgehalten werden.
- Die eingesetzten IT-Systeme SOLLTEN vom Webhoster regelmäßig kontrolliert und gewartet werden. Der Webhoster SOLLTE dazu verpflichtet werden, bei technischen Problemen oder einer Kompromittierung von Kundschaftssystemen zeitnah zu reagieren.
- Der Webhoster SOLLTE grundlegende technische und organisatorische Maßnahmen umsetzen, um seinen Informationsverbund zu schützen.

APP.3.2.A12 Geeigneter Umgang mit Fehlern und Fehlermeldungen (S)

Aus den HTTP-Informationen und den angezeigten Fehlermeldungen SOLLTEN weder der Produktname noch die verwendete Version des Webservers ersichtlich sein. Fehlermeldungen SOLLTEN keine Details zu Systeminformationen oder Konfigurationen ausgeben. Der IT-Betrieb SOLLTE sicherstellen, dass der Webserver ausschließlich allgemeine Fehlermeldungen ausgibt, die Clients darauf hinweisen, dass ein Fehler aufgetreten ist. Die Fehlermeldung SOLLTE ein eindeutiges Merkmal enthalten, das es dem IT-Betrieb ermöglicht, den Fehler nachzuvollziehen. Bei unerwarteten Fehlern SOLLTE sichergestellt sein, dass der Webserver nicht in einem Zustand verbleibt, in dem er anfällig für Angriffe ist.

APP.3.2.A13 Zugriffskontrolle für Webcrawler (S)

Der Zugriff von Webcrawlern SOLLTE nach dem Robots-Exclusion-Standard geregelt werden. Inhalte SOLLTEN mit einem Zugriffsschutz versehen werden, um sie vor Webcrawlern zu schützen, die sich nicht an diesen Standard halten.

APP.3.2.A14 Integritätsprüfungen und Schutz vor Schadsoftware (S)

Der IT-Betrieb SOLLTE regelmäßig prüfen, ob die Konfigurationen des Webservers und die von ihm bereitgestellten Dateien noch integer sind und nicht durch Angriffe verändert wurden. Die zur Veröffentlichung vorgesehenen Dateien SOLLTEN regelmäßig auf Schadsoftware geprüft werden.

APP.3.2.A16 Penetrationstest und Revision (S)

Webserver SOLLTEN regelmäßig auf Sicherheitsprobleme hin überprüft werden. Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert, ausreichend geschützt und vertraulich behandelt werden. Abweichungen SOLLTE nachgegangen werden. Die Ergebnisse SOLLTEN dem ISB vorgelegt werden.

APP.3.2.A20 Benennung von Anzusprechenden (S) [Zentrale Verwaltung]

Bei umfangreichen Webangeboten SOLLTE die Institution zentrale Anzusprechende für die Webangebote bestimmen. Es SOLLTEN Prozesse, Vorgehensweisen und Zuständige für Probleme oder Sicherheitsvorfälle benannt werden.

Die Institution SOLLTE eine Kontaktmöglichkeit auf ihrer Webseite veröffentlichen, über die Sicherheitsprobleme an die Institution gemeldet werden können. Für die Behandlung von externen Sicherheitsmeldungen SOLLTE die Institution Prozesse definieren.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.2.A15 Redundanz (H)

Webserver SOLLTEN redundant ausgelegt werden. Auch die Internetanbindung des Webservers und weiterer IT-Systeme, wie etwa der Webanwendungsserver, SOLLTEN redundant ausgelegt sein.

APP.3.2.A17 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.3.2.A18 Schutz vor Denial-of-Service-Angriffen (H)

Der Webserver SOLLTE ständig überwacht werden. Des Weiteren SOLLTEN Maßnahmen definiert und umgesetzt werden, die DDoS-Angriffe verhindern oder zumindest abschwächen.

APP.3.2.A19 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende weiterführende Dokumente veröffentlicht, die für den Betrieb von Webservern relevant sein können:

- Migration auf TLS 1.2 – Handlungsleitfaden
- Sicheres Webhosting: Handlungsempfehlung für Webhoster
- Sicheres Bereitstellen von Webangeboten (ISi-Webserver)

Das National Institute of Standards and Technology (NIST) stellt in seinem Dokument „Guideline on Securing Public Web Servers“ Hinweise zur Absicherung von Webservern zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.3 Fileserver

1. Beschreibung

1.1. Einleitung

Ein Fileserver (oder auch Dateiserver) ist ein Server in einem Netz, der Dateien von (internen) Festplatten oder Netzfestplatten für alle zugriffsberechtigten Personen sowie Clients zentral bereitstellt. Die Datenbestände können von den Zugriffsberechtigten genutzt werden, ohne sie z. B. auf Wechseldatenträgern zu transportieren oder per E-Mail zu verteilen. Dadurch, dass die Daten zentral vorgehalten werden, können sie strukturiert und in verschiedenen Verzeichnissen und Dateien bereitgestellt werden. Bei Fileservern können Zugriffsrechte auf die Dateien zentral vergeben werden. Auch die Datensicherung kann vereinfacht werden, wenn sich alle Informationen an einer zentralen Stelle befinden.

Ein Fileserver verwaltet meistens Massenspeicher, die mit ihm über Schnittstellen wie SCSI (Small Computer System Interface) oder SAS (Serial Attached SCSI) verbunden sind. Die Speicher befinden sich entweder direkt im Gehäuse des Fileservers oder sind extern angeschlossen. Letzteres wird oft als Directly Attached Storage (DAS) bezeichnet. Ein Fileserver kann auf herkömmlicher Server-Hardware oder einer dedizierten Appliance betrieben werden. Oft können bei großen Datenmengen auch zentrale Storage-Area-Network (SAN)-Speicher über Host-Bus-Adapter (HBA) im Server und an SAN-Switches angebunden werden.

1.2. Zielsetzung

In diesem Baustein werden wesentliche, für einen Fileserver spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Einsatz beschrieben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.3.*Fileserver* ist auf jeden Fileserver im Informationsverbund einmal anzuwenden.

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die beim Einsatz von Fileservern zu beachten und zu erfüllen sind. Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand des vorliegenden Bausteins, sondern werden im Baustein SYS1.1 *Allgemeiner Server* bzw. in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt, z. B. in SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server*. Es werden keine Anforderungen an netzbasierte Speichersysteme bzw. Speichernetze beschrieben. Diese sind im Baustein SYS.1.8 *Speicherlösungen* zu finden. Auch wird nicht auf dedizierte Dienste eingegangen, mit denen ein Fileserver betrieben werden kann, wie z. B. Samba. Der Dienst Samba wird im Baustein APP.3.4 *Samba* behandelt.

Ein wichtiger Schwerpunkt bei der Absicherung eines Fileservers ist es, Zugriffsrechte auf Dateien nur restriktiv zu vergeben. Weitergehende Anforderungen hierzu sind in dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden. Auch die Sicherung der auf einem Fileserver abgelegten Informationen wird in diesem Baustein nicht behandelt. Hierzu sind die Anforderungen des Bausteins CON.3 *Datensicherungskonzept* zu erfüllen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.3 *Fileserver* von besonderer Bedeutung.

2.1. Ausfall eines Fileservers

Fällt ein Fileserver aus, kann der gesamte Informationsverbund davon betroffen sein und damit auch wichtige Geschäftsprozesse und Fachaufgaben der Institution. Nicht nur Benutzende, sondern auch Anwendungen können auf Daten vom Fileserver angewiesen sein, um ordnungsgemäß zu funktionieren. Ist die Verfügbarkeit von Daten und Diensten nicht gegeben, können z. B. Fristen nicht eingehalten oder essenzielle Geschäftsprozesse unterbrochen werden. Ist zudem kein Notfallmanagementkonzept vorhanden, können sich Wiederanlaufzeiten weiter erhöhen. In vielen Fällen führt dies zu finanziellen Einbußen. Außerdem kann sich der Ausfall auf andere Institutionen auswirken.

2.2. Unzureichende Dimensionierung des Fileservers

Ist die Leitungsanbindung oder die Speicherkapazität des Fileservers unzureichend, können sich die Zugriffszeiten erhöhen oder Speicherengpässe können auftreten. Dadurch können beispielsweise Mitarbeitende aufgrund der längeren Wartezeiten frustriert werden und damit beginnen, Daten lokal zu speichern. So kann nicht mehr nachvollzogen werden, wo Daten gespeichert sind und wer im Besitz der Daten ist. Auch Applikationen, die auf eine korrekte (Zwischen-)Speicherung von Informationen angewiesen sind, können nicht mehr zuverlässig funktionieren.

2.3. Unzureichende Überprüfung von abgelegten Dateien

Ist ein Fileserver unzureichend in das Konzept zum Schutz vor Schadprogrammen der Institution einbezogen, kann es passieren, dass unbemerkt Schadsoftware auf dem Fileserver abgelegt wird. Alle IT-Systeme und Anwendungen, die auf die Daten des Fileservers zugreifen, können mit der Schadsoftware infiziert werden, wodurch sich die Schadsoftware sehr schnell in der gesamten Institution ausbreitet.

2.4. Fehlendes oder unzureichendes Zugriffsberechtigungskonzept

Werden Zugriffsberechtigungen und Freigaben nicht ordnungsgemäß konzipiert und vergeben, können eventuell Dritte unbefugt auf Daten zugreifen. Dadurch können Unberechtigte Daten verändern, löschen oder kopieren.

2.5. Unstrukturierte Datenhaltung

Wird die Speicherstruktur nicht vorgegeben bzw. halten sich die Mitarbeitenden nicht daran, können Daten unübersichtlich und unkoordiniert auf dem Fileserver gespeichert werden. Das führt zu verschiedenen Problemen, wie zum Beispiel Speicherplatzverschwendung durch das mehrmalige Ablegen derselben Datei. Auch können unterschiedliche Versionen einer Datei abgelegt werden. Außerdem sind unbefugte Zugriffe möglich, wenn sich z. B. Dateien in Verzeichnissen oder Dateisystemen befinden, die Dritten zugänglich gemacht werden.

2.6. Verlust von auf Fileservern abgespeicherten Daten

Fällt ein Fileserver komplett aus oder sind einzelne Komponenten defekt, können ohne eine Dateisynchronisierung oder ein funktionierendes Backup wichtige Informationen verloren gehen. Das gleiche gilt, wenn Mitarbeitende Dateien unbeabsichtigt löschen. Sollte zudem keine ausreichende Redundanz, etwa durch ein geeignetes Redundant Array of Independent Disks (RAID), eingesetzt werden, können weitere Probleme folgen. So wirkt sich der Ausfall eines einzelnen Datenträgers direkt auf den laufenden Betrieb aus, da die Dateien nicht mehr verfügbar sind.

2.7. Ransomware

Eine spezielle Form von Schadprogrammen ist Ransomware, bei der Daten auf den infizierten IT-Systemen verschlüsselt werden. Angreifende verlangen im Nachgang die Zahlung eines Lösegelds, damit das Opfer die Daten wieder entschlüsseln kann. Es ist jedoch auch nach der Zahlung eines Lösegelds nicht gewährleistet, dass die Daten wiederhergestellt werden können.

Nicht nur die lokalen Daten des infizierten IT-Systems werden hierbei verschlüsselt. Viele Ausprägungen von Ransomware suchen nach Netzlaufwerken mit Schreibzugriff, auf denen alle Daten ebenfalls verschlüsselt werden.

Damit können alle verschlüsselten Informationen seit der letzten Datensicherung verloren sein, auch wenn ein Lösegeld gezahlt wurde. Nicht nur das ursprünglich infizierte IT-System wäre hiervon betroffen, sondern auch zentral abgelegte Informationen, auf die viele IT-Systeme zugreifen dürfen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.3 *Fileserver* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.3.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A2 Einsatz von RAID-Systemen (B)

Der IT-Betrieb MUSS festlegen, ob im Fileserver ein RAID-System eingesetzt werden soll. Eine Entscheidung gegen ein solches System MUSS nachvollziehbar dokumentiert werden. Falls ein RAID-System eingesetzt werden soll, MUSS der IT-Betrieb entscheiden:

- welches RAID-Level benutzt werden soll,
- wie lang die Zeitspanne für einen RAID-Rebuild-Prozess sein darf und
- ob ein Software- oder ein Hardware-RAID eingesetzt werden soll.

In einem RAID SOLLTEN Hotspare-Festplatten vorgehalten werden.

APP.3.3.A3 Einsatz von Viren-Schutzprogrammen (B)

Alle Daten MÜSSEN durch ein Viren-Schutzprogramm auf Schadsoftware untersucht werden, bevor sie auf dem Fileserver abgelegt werden.

APP.3.3.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A15 Planung von Fileservern (B)

Bevor eine Institution einen oder mehrere Fileserver einführt, SOLLTE sie entscheiden, wofür die Fileserver genutzt und welche Informationen darauf verarbeitet werden. Die Institution SOLLTE jede benutzte Funktion eines Fileservers einschließlich deren Sicherheitsaspekte planen. Arbeitsplatzrechner DÜRFEN NICHT als Fileserver eingesetzt werden.

Der Speicherplatz des Fileservers MUSS ausreichend dimensioniert sein. Auch ausreichende Speicherreserven SOLLTEN vorgehalten werden. Es SOLLTE ausschließlich Massenspeicher verwendet werden, der für einen Dauerbetrieb

ausgelegt ist. Die Geschwindigkeit und die Anbindung der Massenspeicher MUSS für den Einsatzzweck angemessen sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.3.A6 Beschaffung eines Fileservers und Auswahl eines Dienstes (S)

Die Fileserver-Software SOLLTE geeignet ausgewählt werden. Der Fileserver-Dienst SOLLTE den Einsatzzweck des Fileservers unterstützen, z. B. Einbindung von Netzlaufwerken in den Clients, Streaming von Multimedia-Inhalten, Übertragung von Boot-Images von festplattenlosen IT-Systemen oder ausschließliche Dateiübertragung über FTP. Die Leistung, die Speicherkapazität, die Bandbreite sowie die Anzahl der Benutzenden, die den Fileserver nutzen, SOLLTEN bei der Beschaffung des Fileservers berücksichtigt werden.

APP.3.3.A7 Auswahl eines Dateisystems (S)

Der IT-Betrieb SOLLTE eine Anforderungsliste erstellen, nach der die Dateisysteme des Fileservers bewertet werden. Das Dateisystem SOLLTE den Anforderungen der Institution entsprechen. Das Dateisystem SOLLTE eine Journaling-Funktion bieten. Auch SOLLTE es über einen Schutzmechanismus verfügen, der verhindert, dass mehrere Benutzende oder Anwendungen gleichzeitig schreibend auf eine Datei zugreifen.

APP.3.3.A8 Strukturierte Datenhaltung (S) [Benutzende]

Es SOLLTE eine Struktur festgelegt werden, nach der Daten abzulegen sind. Die Benutzenden SOLLTEN regelmäßig über die geforderte strukturierte Datenhaltung informiert werden. Die Dateien SOLLTEN ausschließlich strukturiert auf den Fileserver abgelegt werden. Es SOLLTE schriftlich festgelegt werden, welche Daten lokal und welche auf dem Fileserver gespeichert werden dürfen. Programm- und Arbeitsdaten SOLLTEN in getrennten Verzeichnissen gespeichert werden. Die Institution SOLLTE regelmäßig überprüfen, ob die Vorgaben zur strukturierten Datenhaltung eingehalten werden.

APP.3.3.A9 Sicheres Speichermanagement (S)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, ob die Massenspeicher des Fileservers noch wie vorgesehen funktionieren. Es SOLLTEN geeignete Ersatzspeicher vorgehalten werden.

Wurde eine Speicherhierarchie (Primär-, Sekundär- bzw. Tertiärspeicher) aufgebaut, SOLLTE ein (teil-)automatisiertes Speichermanagement verwendet werden. Werden Daten automatisiert verteilt, SOLLTE regelmäßig manuell überprüft werden, ob dies korrekt funktioniert.

Es SOLLTEN mindestens nicht-autorisierte Zugriffsversuche auf Dateien und Änderungen von Zugriffsrechten protokolliert werden.

APP.3.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.3.A11 Einsatz von Speicherbeschränkungen (S)

Der IT-Betrieb SOLLTE bei mehreren Benutzenden auf dem Fileserver prüfen, Beschränkungen des Speicherplatzes für einzelne Benutzende (Quotas) einzurichten. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystems genutzt werden, um die Benutzenden bei einem bestimmten Füllstand der Festplatte zu warnen oder in diesem Fall nur noch dem IT-Betrieb Schreibrechte einzuräumen.

APP.3.3.A14 Einsatz von Error-Correction-Codes (S)

Der IT-Betrieb SOLLTE ein fehlererkennendes bzw. fehlerkorrigierendes Dateisystem einsetzen. Hierfür SOLLTE genügend Speicherplatz vorgehalten werden. Der IT-Betrieb SOLLTE beachten, dass, je nach eingesetztem Verfahren, Fehler nur mit einer gewissen Wahrscheinlichkeit erkannt und auch nur in begrenzter Größenordnung behoben werden können.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.3.A12 Verschlüsselung des Datenbestandes (H)

Die Massenspeicher des Fileservers SOLLTEN auf Dateisystem- oder Hardwareebene verschlüsselt werden. Falls Hardwareverschlüsselung eingesetzt wird, SOLLTEN Produkte verwendet werden, deren Verschlüsselungsfunktion zertifiziert wurde. Es SOLLTE sichergestellt werden, dass der Virenschutz die verschlüsselten Daten auf Schadsoftware prüfen kann.

APP.3.3.A13 Replikation zwischen Standorten (H)

Für hochverfügbare Fileserver SOLLTE eine angemessene Replikation der Daten auf mehreren Massenspeichern stattfinden. Daten SOLLTEN zudem zwischen unabhängigen Fileservern repliziert werden, die sich an unabhängigen Standorten befinden. Dafür SOLLTE vom IT-Betrieb ein geeigneter Replikationsmechanismus ausgewählt werden. Damit die Replikation wie vorgesehen funktionieren kann, SOLLTEN hinreichend genaue Zeitdienste genutzt und betrieben werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.3.3 *Fileserver* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.4 Samba

1. Beschreibung

1.1. Einleitung

Samba ist ein frei verfügbarer und vollwertiger Active Directory Domain Controller (ADDC), der Authentisierungs-, Datei- und Druckdienste bereitstellen kann und dadurch die Interoperabilität zwischen der Windows- und der Unix-Welt ermöglicht. Samba führt viele unterschiedliche Protokolle und Techniken zusammen. Dazu gehört beispielsweise das Server-Message-Block (SMB)-Protokoll. Als Samba-Server werden Server bezeichnet, auf denen Samba betrieben wird. In der Regel sind das Unix-Server.

Wurde der Einsatz von Samba korrekt konzipiert und geeignet konfiguriert, interagiert Samba mit einem Windows-Client oder -Server, als ob es selbst ein Windows-System wäre.

1.2. Zielsetzung

Ziel des Bausteins ist es darzustellen, wie Samba in Institutionen sicher eingesetzt werden kann und wie sich die durch Samba bereitgestellten Informationen schützen lassen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.4.*Samba* ist auf jeden Samba-Server des betrachteten Informationsverbunds anzuwenden.

Dieser Baustein betrachtet Samba als Authentisierungs-, Datei- und Druckdienst. Da Samba in der Regel auf Unix-Servern eingesetzt wird und dort aus der Windows-Server-Welt bekannte Dienste bereitstellt, sind die Sicherheitsaspekte der Bausteine SYS.1.1 *Allgemeiner Server* und SYS.1.3 *Server unter Linux und Unix* zu berücksichtigen.

Ein wichtiger Schwerpunkt bei der Absicherung eines Samba-Servers ist es, Zugriffsrechte auf Dateien nur restriktiv zu vergeben. Vertiefende Informationen zum Identitäts- und Berechtigungsmanagement sind nicht in diesem Baustein, sondern in ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden.

Generelle Sicherheitsanforderungen für Drucker, Fileserver oder Verzeichnisdienste sind nicht Bestandteil dieses Bausteins. Diese werden in den Bausteinen SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte*, APP.3.3 *Fileserver* und APP.2.1 *Allgemeiner Verzeichnisdienst* sowie APP.2.3 *OpenLDAP* beschrieben.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.4 *Samba* von besonderer Bedeutung.

2.1. Abhören ungeschützter Kommunikationsverbindungen von Samba

Wenn ungeschützte Kommunikationsverbindungen von Samba abgehört werden, können vertrauliche Informationen abgefangen und missbraucht werden. Beim Dateitransfer zwischen Unix-Servern, Windows-Servern und Clients werden oftmals Protokolle ohne umfangreiche Sicherheitseigenschaften eingesetzt, sodass sowohl Authentisierungs- als auch Nutzungsdaten für Dritte zugänglich sind und von Unberechtigten missbraucht werden könnten. Das kann dazu führen, dass schützenswerte Informationen der Institution in die falschen Hände gelangen.

2.2. Unsichere Standardeinstellungen auf Samba-Servern

Um einige Fähigkeiten des Samba-Servers zu zeigen und um den Administrierenden einen schnellen Einstieg zu ermöglichen, wird während der Installation des Samba-Servers die Konfigurationsdatei smb.conf mit Standardeinstellungen erzeugt. Mit den in dieser Datei voreingestellten Optionen kann der Samba-Server im Anschluss gestartet werden. Wird diese Datei unbedacht ohne weitere Anpassungen benutzt, kann das zu erheblichen Sicherheitslücken führen. Werden die beispielhaft vorgenommenen Dateifreigaben nicht auskommentiert, können in diesen unerwünschten Freigaben sensible Informationen eingesehen werden.

2.3. Unberechtigte Nutzung oder Administration von Samba

Unbefugte können durch die Nutzung von Anwendungen oder IT-Systemen an vertrauliche Informationen gelangen, diese manipulieren oder Störungen verursachen. So ist es möglich, dass sie Samba unberechtigt administrieren können. Besonders kritisch ist es, wenn veraltete und nicht mehr aktualisierte Konfigurationswerkzeuge eingesetzt werden, wie z. B. das Samba Web Administration Tool (SWAT).

2.4. Fehlerhafte Administration von Samba

Sind die Administrierenden mit den umfangreichen Komponenten, Funktionen, Optionen und Konfigurationseinstellungen von Samba zu wenig vertraut, kann dies zu weitreichenden Komplikationen führen. So können Fehlkonfigurationen des DNS oder des Berechtigungsmanagements dazu führen, dass Unbefugte auf Ressourcen zugreifen können. Des Weiteren kann dies zu Betriebsunterbrechungen führen oder es können schützenswerte Informationen offengelegt werden.

2.5. Datenverlust bei Samba

Ein Datenverlust wirkt sich erheblich auf den IT-Einsatz aus. Wenn institutionsrelevante Informationen zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder gar nicht mehr ausgeführt werden. Bei Samba ist beispielsweise zu beachten, dass sich die Eigenschaften der Dateisysteme unter Windows und Unix erheblich voneinander unterscheiden. Deswegen ist nicht immer sichergestellt, dass die Zugriffsrechte unter Windows aufrechterhalten bleiben, unter Umständen können so wichtige Dateieigenschaften verloren gehen. Auch können dadurch Informationen zu sogenannten Alternate Data Streams (ADS) und DOS-Attributen verloren gehen.

2.6. Integritätsverlust schützenswerter Informationen bei Samba

Samba selbst legt wichtige Betriebsdaten in Datenbanken im Trivial-Database-(TDB)-Format ab. Sollten diese Datenbanken vom Betriebssystem nicht ausreichend leistungsfähig und konsistent behandelt werden, können sie Probleme verursachen, wenn Samba-Dienste genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.4 *Samba* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.4.A1 Planung des Einsatzes eines Samba-Servers (B)

Der IT-Betrieb MUSS die Einführung eines Samba-Servers sorgfältig planen und regeln. Der IT-Betrieb MUSS abhängig vom Einsatzszenario definieren, welche Aufgaben der Samba-Server zukünftig erfüllen soll und in welcher Betriebsart er betrieben wird. Außerdem MUSS festgelegt werden, welche Komponenten von Samba und welche weiteren Komponenten dafür erforderlich sind.

Soll die Cluster-Lösung CTDB (Cluster Trivia Data Base) eingesetzt werden, MUSS der IT-Betrieb diese Lösung sorgfältig konzeptionieren. Falls Samba die Active-Directory-(AD)-Dienste auch für Linux- und Unix-Systeme bereitstellen soll, MÜSSEN diese Dienste ebenfalls sorgfältig geplant und getestet werden. Des Weiteren MUSS das Authentisierungsverfahren für das AD sorgfältig konzipiert und implementiert werden. Die Einführung und die Reihenfolge, in der die Stackable-Virtual-File-System-(VFS)-Module ausgeführt werden, MUSS sorgfältig konzipiert werden. Die Umsetzung SOLLTE dokumentiert werden.

Soll IPv6 unter Samba eingesetzt werden, MUSS auch dies sorgfältig geplant werden. Zudem MUSS in einer betriebsnahen Testumgebung überprüft werden, ob die Integration fehlerfrei funktioniert.

APP.3.4.A2 Sichere Grundkonfiguration eines Samba-Servers (B)

Der IT-Betrieb MUSS den Samba-Server sicher konfigurieren. Hierfür MÜSSEN unter anderem die Einstellungen für die Zugriffskontrollen angepasst werden. Das gleiche SOLLTE auch für Einstellungen gelten, welche die Leistungsfähigkeit des Servers beeinflussen.

Samba MUSS vom IT-Betrieb so konfiguriert werden, dass Verbindungen nur von sicheren Hosts und Netzen entgegengenommen werden. Änderungen an der Konfiguration SOLLTEN sorgfältig dokumentiert werden, sodass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat. Dabei MUSS nach jeder Änderung überprüft werden, ob die Syntax der Konfigurationsdatei noch korrekt ist.

Zusätzliche Softwaremodule wie SWAT DÜRFEN NICHT installiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.4.A3 Sichere Konfiguration eines Samba-Servers (S)

Datenbanken im Trivial-Database-(TDB)-Format SOLLTEN NICHT auf einer Partition gespeichert werden, die ReiserFS als Dateisystem benutzt. Wird eine netlogon-Freigabe konfiguriert, SOLLTEN unberechtigte Benutzende KEINE Dateien in dieser Freigabe modifizieren können.

Das Betriebssystem eines Samba-Servers SOLLTE Access Control Lists (ACLs) in Verbindung mit dem eingesetzten Dateisystem unterstützen. Zusätzlich SOLLTE sichergestellt werden, dass das Dateisystem mit den passenden Parametern eingebunden wird.

Die Voreinstellungen von SMB Message Signing SOLLTEN beibehalten werden, sofern sie nicht im Widerspruch zu den existierenden Sicherheitsrichtlinien im Informationsverbund stehen.

APP.3.4.A4 Vermeidung der NTFS-Eigenschaften auf einem Samba-Server (S)

Wird eine Version von Samba eingesetzt, die im New Technology File System (NTFS) keine ADS abbilden kann und sollen Dateisystemobjekte über Systemgrenzen hinweg kopiert oder verschoben werden, SOLLTEN Dateisystemobjekte KEINE ADS mit wichtigen Informationen enthalten.

APP.3.4.A5 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server (S)

Die von Samba standardmäßig verwendeten Parameter, mit denen DOS-Attribute auf das Unix-Dateisystem abgebildet werden, SOLLTEN NICHT verwendet werden. Stattdessen SOLLTE Samba so konfiguriert werden, dass es DOS-Attribute und die Statusindikatoren zur Vererbung (Flag) in Extended Attributes speichert. Die Freigaben SOLLTEN ausschließlich über die Samba-Registry verwaltet werden.

Ferner SOLLTEN die effektiven Zugriffsberechtigungen auf die Freigaben des Samba-Servers regelmäßig überprüft werden.

APP.3.4.A6 Sichere Konfiguration von Winbind unter Samba (S)

Für jedes Domänen-Konto einer Windows-Domäne SOLLTE im Betriebssystem des Servers ein Konto mit allen notwendigen Gruppenmitgliedschaften vorhanden sein. Falls das nicht möglich ist, SOLLTE Winbind eingesetzt werden, um Domänen-Konten in Unix-Konten umsetzen. Beim Einsatz von Winbind SOLLTE sichergestellt werden, dass Kollisionen zwischen lokalen Benutzenden in Unix und Benutzenden in der Domäne verhindert werden.

Des Weiteren SOLLTEN die PAM (Pluggable Authentication Modules) eingebunden werden.

APP.3.4.A7 Sichere Konfiguration von DNS unter Samba (S)

Wenn Samba als DNS-Server eingesetzt wird, SOLLTE die Einführung sorgfältig geplant und die Umsetzung vorab getestet werden. Da Samba verschiedene AD-Integrationsmodi unterstützt, SOLLTE der IT-Betrieb die DNS-Einstellungen entsprechend dem Verwendungsszenario von Samba vornehmen.

APP.3.4.A8 Sichere Konfiguration von LDAP unter Samba (S)

Werden die Benutzenden unter Samba mit LDAP verwaltet, SOLLTE die Konfiguration sorgfältig vom IT-Betrieb geplant und dokumentiert werden. Die Zugriffsberechtigungen auf das LDAP SOLLTEN mittels ACLs geregelt werden.

APP.3.4.A9 Sichere Konfiguration von Kerberos unter Samba (S)

Zur Authentisierung SOLLTE das von Samba implementierte Heimdal Kerberos Key Distribution Center (KDC) verwendet werden. Es SOLLTE darauf geachtet werden, dass die von Samba vorgegebene Kerberos-Konfigurationsdatei verwendet wird. Es SOLLTEN nur sichere Verschlüsselungsverfahren für Kerberos-Tickets benutzt werden.

Wird mit Kerberos authentisiert, SOLLTE der zentrale Zeitserver lokal auf dem Samba-Server installiert werden. Der NTP-Dienst SOLLTE so konfiguriert werden, dass nur autorisierte Clients die Zeit abfragen können.

APP.3.4.A10 Sicherer Einsatz externer Programme auf einem Samba-Server (S)

Vom IT-Betrieb SOLLTE sichergestellt werden, dass Samba nur auf schadhafte Funktionen überprüfte und vertrauenswürdige externe Programme aufruft.

APP.3.4.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.4.A12 Schulung der Administrierenden eines Samba-Servers (S)

Die Administrierenden SOLLTEN zu den genutzten spezifischen Bereichen von Samba wie z. B. Benutzendenauthentisierung, Windows- und Unix-Rechtemodelle, aber auch zu NTFS ACLs und NTFS ADS geschult werden.

APP.3.4.A13 Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers (S)

Es SOLLTEN alle Systemkomponenten in das institutionsweite Datensicherungskonzept eingebunden werden, die erforderlich sind, um einen Samba-Server wiederherzustellen. Auch die Kontoinformationen aus allen eingesetzten Backends SOLLTEN berücksichtigt werden. Ebenso SOLLTEN alle TDB-Dateien gesichert werden. Des Weiteren SOLLTE die Samba-Registry mit gesichert werden, falls sie für Freigaben eingesetzt wurde.

APP.3.4.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.4.A15 Verschlüsselung der Datenpakete unter Samba (H)

Um die Sicherheit der Datenpakete auf dem Transportweg zu gewährleisten, SOLLTEN die Datenpakete mit den ab SMB Version 3 integrierten Verschlüsselungsverfahren verschlüsselt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.3.4 *Samba* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.6 DNS-Server

1. Beschreibung

1.1. Einleitung

Domain Name System (DNS) ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. DNS kann mit einem Telefonbuch verglichen werden, das Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Üblicherweise wird über DNS zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet.

Welche Hostnamen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für das IT-System benutzt, auf dem diese Software betrieben wird.

DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch häufig im internen Netz einer Institution eingesetzt. Auf den IT-Systemen der Benutzenden sind standardmäßig sogenannte Resolver installiert. Über den Resolver werden die Anfragen an DNS-Server gestellt. Als Antwort liefern die DNS-Server Informationen über den Domain-Namensraum zurück.

DNS-Server können nach ihren Aufgaben unterschieden werden. Dabei gibt es grundsätzlich zwei verschiedenen Typen: Advertising DNS-Server und Resolving DNS-Server. Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz einer Institution.

Der Ausfall eines DNS-Servers kann sich gravierend auf den Betrieb einer IT-Infrastruktur auswirken. Dabei ist nicht das ausgefallene DNS-System an sich problematisch, sondern die DNS-basierten Dienste, die daraus eingeschränkt werden. Unter Umständen sind Webserver oder E-Mail-Server nicht mehr erreichbar oder die Fernwartung funktioniert nicht mehr. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede Zone betrieben werden.

1.2. Zielsetzung

In diesem Baustein werden die für einen DNS-Server spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Einsatz beschrieben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.6 *DNS-Server* ist auf jeden im Informationsverbund eingesetzten DNS-Server anzuwenden.

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn eine Institution DNS-Server einsetzt. Der Fokus liegt dabei auf der Verfügbarkeit von DNS-Servern und der Integrität der übertragenen Informationen. Außerdem werden Probleme behandelt, die auftreten können, wenn DNS-Server eingesetzt werden.

Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand dieses Bausteins. Diese werden im Baustein SYS1.1 *Allgemeiner Server* und in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt, z. B. SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server.*

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.6 *DNS-Server* von besonderer Bedeutung.

2.1. Ausfall des DNS-Servers

Fällt ein DNS-Server aus, kann der gesamte IT-Betrieb davon betroffen sein. Da Clients und andere Server der Institution dann nicht mehr in der Lage sind, interne und externe Adressen auf Basis der Hostnamen aufzulösen, können keine Datenverbindungen mehr aufgebaut werden. Auch externe IT-Systeme, z. B. von mobilen Mitarbeitenden, der Kundschaft sowie Geschäftspartnern und Geschäftspartnerinnen, können nicht auf die Server der Institution zugreifen. Dadurch sind in der Regel essenzielle Geschäftsprozesse gestört.

2.2. Unzureichende Leitungskapazitäten

Reichen die Leitungskapazitäten für einen DNS-Server nicht aus, können sich die Zugriffszeiten auf interne und externe Dienste erhöhen. Dadurch sind diese eventuell nur eingeschränkt oder gar nicht mehr nutzbar. Auch kann der DNS-Server dann leichter durch einen Denial-of-Service-(DoS)-Angriff überlastet werden.

2.3. Fehlende oder unzureichende Planung des DNS-Einsatzes

Fehler in der Planung stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der DNS-Einsatz nicht oder nur unzureichend geplant, kann dies zu Problemen und Sicherheitslücken im laufenden Betrieb führen. Sind beispielsweise die Firewall-Regeln, die den DNS-Verkehr steuern, zu freizügig definiert, kann dies unter Umständen einen Angriff zur Folge haben. Sind die Regeln jedoch zu restriktiv formuliert, können legitime Clients keine Anfragen an die DNS-Server stellen und werden beeinträchtigt, wenn sie etwa Dienste wie E-Mail oder FTP benutzen.

2.4. Fehlerhafte Domain-Informationen

Selbst wenn der DNS-Einsatz sorgfältig geplant und somit alle sicherheitsrelevanten Punkte berücksichtigt wurden, ist das nicht ausreichend, wenn semantisch sowie syntaktisch fehlerhafte Domain-Informationen erstellt werden. Dies gilt beispielsweise dann, wenn einem Hostnamen eine falsche IP-Adresse zugeordnet wird, Daten fehlen, nicht erlaubte Zeichen verwendet werden oder die Vorwärts- und Rückwärtsauflösung inkonsistent sind. Enthalten Domain-Informationen Fehler, funktionieren Dienste, die diese Informationen benutzen, aufgrund der Falschinformationen nur eingeschränkt.

2.5. Fehlerhafte Konfiguration eines DNS-Servers

Sicherheitskritische Standardeinstellungen, selbst konfigurierte sicherheitskritische Einstellungen oder fehlerhafte Konfigurationen können dazu führen, dass ein DNS-Server nicht ordnungsgemäß funktioniert. Ist beispielsweise ein Resolving DNS-Server so konfiguriert, dass er rekursive Anfragen uneingeschränkt entgegennimmt, also sowohl aus dem internen Datennetz als auch aus dem Internet, kann aufgrund der erhöhten Last die Verfügbarkeit des Servers stark beeinträchtigt sein. Zusätzlich könnte er dadurch anfällig für DNS-Reflection-Angriffe werden.

Ebenso besteht bei fehlerhaft konfigurierten DNS-Servern die Gefahr, dass die Zonentransfers nicht auf berechtigte DNS-Server beschränkt sind. Damit kann jeder Host, der die Möglichkeit hat, eine Anfrage an die DNS-Server zu stellen, die gesamten Domain-Informationen dieser Server auslesen. Die so gewonnenen Daten können spätere Angriffe erleichtern.

2.6. DNS-Manipulation

Mit einem DNS-Cache-Poisoning-Angriff wird das Ziel verfolgt, dass das angegriffene IT-System falsche Zuordnungen von IP-Adressen und Namen speichert. Dabei wird ausgenutzt, dass DNS-Server erhaltene Domain-Informationen für einen gewissen Zeitraum im Cache zwischenspeichern. So können sich gefälschte Daten weiträumig verbreiten. Werden dann entsprechende Anfragen an den manipulierten DNS-Server gestellt, liefert dieser als Antwort die gefälschten Daten. Das IT-System, das diese Antwort empfängt, speichert diese zwischen und sein Cache ist somit ebenfalls „vergiftet". Die gespeicherten Daten haben eine definierte Haltbarkeit (Time-To-Live, TTL). Wird

der Resolving DNS-Server nach einer manipulierten Adresse gefragt, so wird er erst dann wieder einen anderen DNS-Server anfragen, wenn die Haltbarkeit abgelaufen ist. So können sich manipulierte DNS-Informationen lange halten, obwohl sie auf dem ursprünglich angegriffenen DNS-Server bereits wieder korrigiert sind. Gelingt es Angreifenden beispielsweise, die Namensauflösung für eine Domain zu übernehmen, indem sie die Einträge so manipulieren, dass ihre DNS-Server befragt werden, sind alle Subdomains automatisch mitbetroffen. DNS-Cache-Poisoning-Angriffe werden oft mit dem Ziel geführt, Anfragen auf bösartige Server umzuleiten.

2.7. DNS-Hijacking

DNS-Hijacking ist eine Angriffsmethode, die verwendet wird, um die Kommunikation zwischen Advertising DNS-Servern und Resolvern über das IT-System der Angreifenden zu leiten. Den Angreifenden ist es mit dieser Man-in-the-Middle-Attacke möglich, die Kommunikation zwischen den Servern abzuhören und aufzuzeichnen. Die weitaus größere Gefahr besteht jedoch darin, dass bei einem erfolgreichen Angriff jeglicher Datenverkehr zwischen den beiden IT-Systemen beliebig verändert werden kann. Wird nach einem erfolgreichen DNS-Hijacking-Angriff vom Resolver eines Clients eine Anfrage an einen DNS-Server gesendet, können Angreifende beispielsweise die Zuordnung von Namen und IP-Adresse ändern. DNS-Hijacking lässt sich auch mit anderen Angriffen kombinieren, zum Beispiel mit Phishing.

2.8. DNS-DoS

Bei einem DoS-Angriff auf einen DNS-Server werden so viele Anfragen an ihn gesendet, dass die Netzverbindung zum DNS-Server bzw. der DNS-Server selbst überlastet wird. In der Regel werden die Anfragen über Botnetze versendet, um die notwendige Datenrate zu erreichen. Ein auf diese Weise überlasteter DNS-Server kann keine legitimen Anfragen mehr beantworten.

2.9. DNS-Reflection

Bei einem DNS-Reflection-Angriff handelt es sich um einen DoS-Angriff, bei dem nicht der DNS-Server, an den die Anfragen gestellt werden, das Ziel ist, sondern das IT-System, das die Antworten empfängt. Dabei wird ausgenutzt, dass bestimmte Anfragen eine verhältnismäßig große Antwortdatenmenge erzeugen. Es ist dabei möglich, einen Verstärkungsfaktor von 100 und mehr zu erreichen. Das bedeutet, dass die Antwort, gemessen in Bytes, mindestens einhundert Mal größer ist als die Anfrage. Durch die Anzahl und Größe der Antworten wird die Netzbandbreite bzw. das empfangende IT-System selbst über seine Leistungskapazität hinaus überlastet. Somit kann jede beliebige technische IT-Komponente das Angriffsziel sein. DNS-Reflection-Angriffe werden durch Open Resolver begünstigt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.6 *DNS-Server* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Zentrale Verwaltung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.6.A1 Planung des DNS-Einsatzes (B)

Der Einsatz von DNS-Servern MUSS sorgfältig geplant werden. Es MUSS zuerst festgelegt werden, wie der Netzdienst DNS aufgebaut werden soll. Es MUSS festgelegt werden, welche Domain-Informationen schützenswert sind. Es MUSS geplant werden, wie DNS-Server in das Netz des Informationsverbunds eingebunden werden sollen. Die getroffenen Entscheidungen MÜSSEN geeignet dokumentiert werden.

APP.3.6.A2 Einsatz redundanter DNS-Server (B)

Advertising DNS-Server MÜSSEN redundant ausgelegt werden. Für jeden Advertising DNS-Server MUSS es mindestens einen zusätzlichen Secondary DNS-Server geben.

APP.3.6.A3 Verwendung von separaten DNS-Servern für interne und externe Anfragen (B)

Advertising DNS-Server und Resolving DNS-Server MÜSSEN serverseitig getrennt sein. Die Resolver der internen IT-Systeme DÜRFEN NUR die internen Resolving DNS-Server verwenden.

APP.3.6.A4 Sichere Grundkonfiguration eines DNS-Servers (B)

Ein Resolving DNS-Server MUSS so konfiguriert werden, dass er ausschließlich Anfragen aus dem internen Netz akzeptiert. Wenn ein Resolving DNS-Server Anfragen versendet, MUSS er zufällige Source Ports benutzen. Sind DNS-Server bekannt, die falsche Domain-Informationen liefern, MUSS der Resolving DNS-Server daran gehindert werden, Anfragen dorthin zu senden. Ein Advertising DNS-Server MUSS so konfiguriert werden, dass er Anfragen aus dem Internet immer iterativ behandelt.

Es MUSS sichergestellt werden, dass DNS-Zonentransfers zwischen Primary und Secondary DNS-Servern funktionieren. Zonentransfers MÜSSEN so konfiguriert werden, dass diese nur zwischen Primary und Secondary DNS-Servern möglich sind. Zonentransfers MÜSSEN auf bestimmte IP-Adressen beschränkt werden. Die Version des verwendeten DNS-Server-Produktes MUSS verborgen werden.

APP.3.6.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.6.A6 Absicherung von dynamischen DNS-Updates (B)

Es MUSS sichergestellt werden, dass nur legitimierte IT-Systeme Domain-Informationen ändern dürfen. Es MUSS festgelegt werden, welche Domain-Informationen die IT-Systeme ändern dürfen.

APP.3.6.A7 Überwachung von DNS-Servern (B)

DNS-Server MÜSSEN laufend überwacht werden. Es MUSS überwacht werden, wie ausgelastet die DNS-Server sind, um rechtzeitig die Leistungskapazität der Hardware anpassen zu können. DNS-Server MÜSSEN so konfiguriert werden, dass mindestens die folgenden sicherheitsrelevanten Ereignisse protokolliert werden:

- Anzahl der DNS-Anfragen,
- Anzahl der Fehler bei DNS-Anfragen,
- EDNS-Fehler (EDNS – Extension Mechanisms for DNS),
- auslaufende Zonen sowie
- fehlgeschlagene Zonentransfers.

APP.3.6.A8 Verwaltung von Domainnamen (B) [Zentrale Verwaltung]

Es MUSS sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Institution benutzt werden, regelmäßig und rechtzeitig verlängert werden. Eine Person MUSS bestimmt werden, die dafür zuständig ist, die Internet-Domainnamen zu verwalten. Falls Dienstleistende mit der Domainverwaltung beauftragt werden, MUSS darauf geachtet werden, dass die Institution die Kontrolle über die Domains behält.

APP.3.6.A9 Erstellen eines Notfallplans für DNS-Server (B)

Ein Notfallplan für DNS-Server MUSS erstellt werden. Der Notfallplan für DNS-Server MUSS in die bereits vorhandenen Notfallpläne der Institution integriert werden. Im Notfallplan für DNS-Server MUSS ein Datensicherungskonzept für die Zonen- und Konfigurationsdateien beschrieben sein. Das Datensicherungskonzept für die Zonen- und Konfigurationsdateien MUSS in das existierende Datensicherungskonzept der Institution integriert werden. Der Notfallplan für DNS-Server MUSS einen Wiederanlaufplan für alle DNS-Server im Informationsverbund enthalten.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.6.A10 Auswahl eines geeigneten DNS-Server-Produktes (S)

Wird ein DNS-Server-Produkt beschafft, dann SOLLTE darauf geachtet werden, dass es sich in der Praxis ausreichend bewährt hat. Das DNS-Server-Produkt SOLLTE die aktuellen RFC-Standards unterstützen. Das DNS-Server-Produkt SOLLTE die Zuständigen dabei unterstützen, syntaktisch korrekte Master Files zu erstellen.

APP.3.6.A11 Ausreichende Dimensionierung der DNS-Server (S)

Die Hardware des DNS-Servers SOLLTE ausreichend dimensioniert sein. Die Hardware des DNS-Servers SOLLTE ausschließlich für den Betrieb dieses DNS-Servers benutzt werden. Die Netzanbindungen sämtlicher DNS-Server im Informationsverbund SOLLTEN ausreichend bemessen sein.

APP.3.6.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.6.A13 Einschränkung der Sichtbarkeit von Domain-Informationen (S)

Der Namensraum eines Informationsverbunds SOLLTE in einen öffentlichen und einen institutionsinternen Bereich aufgeteilt werden. Im öffentlichen Teil SOLLTEN nur solche Domain-Informationen enthalten sein, die von Diensten benötigt werden, die von extern erreichbar sein sollen. IT-Systeme im internen Netz SOLLTEN selbst dann keinen von außen auflösbaren DNS-Namen erhalten, wenn sie eine öffentliche IP-Adresse besitzen.

APP.3.6.A14 Platzierung der Nameserver (S)

Primary und Secondary Advertising DNS-Server SOLLTEN in verschiedenen Netzsegmenten platziert werden.

APP.3.6.A15 Auswertung der Logdaten (S)

Die Logdateien des DNS-Servers SOLLTEN regelmäßig überprüft werden. Die Logdateien des DNS-Servers SOLLTEN regelmäßig ausgewertet werden. Mindestens die folgenden sicherheitsrelevanten Ereignisse SOLLTEN ausgewertet werden:

- Anzahl der DNS-Anfragen,
- Anzahl der Fehler bei DNS-Anfragen,
- EDNS-Fehler,
- auslaufende Zonen,
- fehlgeschlagene Zonentransfers sowie
- Veränderungen im Verhältnis von Fehlern zu DNS-Anfragen.

APP.3.6.A16 Integration eines DNS-Servers in eine „P-A-P"-Struktur (S)

Die DNS-Server SOLLTEN in eine „Paketfilter – Application-Level-Gateway – Paketfilter"-(P-A-P)-Struktur integriert werden (siehe auch NET.1.1 *Netzarchitektur und -design*). Der Advertising DNS-Server SOLLTE in diesem Fall in einer demilitarisierten Zone (DMZ) des äußeren Paketfilters angesiedelt sein. Der Resolving DNS-Server SOLLTE in einer DMZ des inneren Paketfilters aufgestellt sein.

APP.3.6.A17 Einsatz von DNSSEC (S)

Die DNS-Protokollerweiterung DNSSEC SOLLTE sowohl auf Resolving DNS-Servern als auch auf Advertising DNS-Servern aktiviert werden. Die dabei verwendeten Schlüssel Key-Signing-Keys (KSK) und Zone-Signing-Keys (ZSK) SOLLTEN regelmäßig gewechselt werden.

APP.3.6.A18 Erweiterte Absicherung von Zonentransfers (S)

Um Zonentransfers stärker abzusichern, SOLLTEN zusätzlich Transaction Signatures (TSIG) eingesetzt werden.

APP.3.6.A19 Aussonderung von DNS-Servern (S)

Der DNS-Server SOLLTE sowohl aus dem Domain-Namensraum als auch aus dem Netzverbund gelöscht werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.6.A20 Prüfung des Notfallplans auf Durchführbarkeit (H)

Es SOLLTE regelmäßig überprüft werden, ob der Notfallplan für DNS-Server durchführbar ist.

APP.3.6.A21 Hidden Master (H)

Um Angriffe auf den primären Advertising DNS-Server zu erschweren, SOLLTE eine sogenannte Hidden-Master-Anordnung vorgenommen werden.

APP.3.6.A22 Anbindung der DNS-Server über unterschiedliche Provider (H)

Extern erreichbare DNS-Server SOLLTEN über unterschiedliche Provider angebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld DNS veröffentlicht:

- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 055: „Sichere Bereitstellung von DNS-Diensten: Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen“
- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 121: „Umsetzung von DNSSEC: Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions“
- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-81-2 „Secure Domain Name System (DNS) – Deployment Guide“ Empfehlungen zum Einsatz von DNS.

Im Request for Comments (RFC) bietet der RFC 1034 „Domain Names – Concepts and Facilities“ weiterführende Informationen zu DNS.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.4.2 SAP-ERP-System

1. Beschreibung

1.1. Einleitung

Enterprise-Resource-Planning-Systeme von SAP (kurz SAP-ERP-Systeme) werden eingesetzt, um interne und externe Geschäftsabläufe zu automatisieren und technisch zu unterstützen. SAP-ERP-Systeme verarbeiten daher typischerweise vertrauliche Informationen, sodass alle Komponenten und Daten geeignet geschützt werden müssen.

SAP-ERP-Systeme sind aktuell unter den Produktbezeichnungen SAP Business Suite und SAP S/4HANA auf dem Markt. Ein SAP-ERP-System setzt sich aus verschiedenen Modulen zusammen, mit denen die Organisationsstruktur einer Institution abgebildet werden kann. Zu den Modulen eines SAP-ERP-Systems zählen unter anderem Rechnungswesen, Personalwirtschaft und Logistik. Die Kernkomponenten des SAP-ERP-Systems sind SAP NetWeaver (Applikationsserver-Middleware) und SAP HANA (Applikationsserver und Datenbank). SAP NetWeaver ermöglicht es, SAP-ABAP- und SAP-JAVA-Anwendungen anzubinden und Prozesse systemweit zu steuern. SAP HANA kann in Echtzeit große Datenmengen für alle Geschäftsbereiche analysieren.

1.2. Zielsetzung

Der Baustein beschreibt, welche Gefährdungen für SAP-ERP-Systeme zu beachten sind und wie diese Systeme sicher installiert, konfiguriert und betrieben werden können. Er richtet sich an Informationssicherheitsbeauftragte und Administrierende, die dafür zuständig sind, SAP-ERP-Systeme zu planen und umzusetzen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.4.2 *SAP-ERP-System* ist auf jedes SAP-ERP-System anzuwenden.

Der Baustein beschränkt sich auf die Kerninstallation eines SAP-ERP-Systems und fokussiert die spezifischen Merkmale des darunterliegenden SAP-NetWeaver-Applikationsservers. Auch werden in diesem Baustein nicht alle verfügbaren SAP-Produkte detailliert beschrieben. Die folgenden Darstellungen beschränken sich auf die Konfiguration der SAP-Basis und gehen nicht auf Module oder Applikationen ein.

Anforderungen an die Entwicklung von ABAP-Programmen finden sich im Baustein APP.4.6 *SAP ABAP-Programmierung*. Darüber hinaus werden keine angrenzenden IT-Systeme, Betriebssysteme oder Datenbanken näher betrachtet. Dazu sind die spezifischen Bausteine wie SYS1.2.2 *Windows Server 2012*, SYS.1.3 *Server unter Linux und Unix* oder APP.4.3 *Relationale Datenbanken* anzuwenden. Ebenso geht der vorliegende Baustein nicht auf SAP HANA ein. Auf aktuelle Bezeichnungen der Produkte wird bewusst verzichtet, da sich diese häufig ändern.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.4.2 *SAP-ERP-System* von besonderer Bedeutung:

2.1. Fehlende Berücksichtigung der Sicherheitsempfehlungen von SAP

Wird ein SAP-ERP-System aufgebaut, ohne dabei die empfohlenen Sicherheitsleitfäden von SAP zu berücksichtigen, kann das zu schweren Sicherheitsproblemen im System führen. Das ist z. B. der Fall, wenn SAP-Empfehlungen für das Konten- und Berechtigungsmanagement nicht korrekt umgesetzt werden. Auch wenn solche SAP-Empfeh-

lungen ignoriert werden, welche die Kommunikation oder den Schnittstellenbetrieb mittels RFC und Webservices schützen, können Schwachstellen auftreten. Dadurch kann das gesamte System angreifbar sein.

2.2. Fehlendes oder nicht zeitnahes Einspielen von Patches und SAP-Sicherheitshinweisen

SAP-ERP-Systeme bestehen aus unterschiedlichen Modulen und Komponenten und sind komplexe Systeme, die meist sensible Daten verarbeiten. SAP veröffentlicht daher regelmäßig Patches und Sicherheitshinweise, um Softwarefehler und bekannt gewordene Schwachstellen zu beheben. Wenn neue Patches oder SAP-Sicherheitshinweise nicht zeitnah oder gar nicht eingespielt werden, könnten offene Sicherheitslücken von Angreifenden ausgenutzt werden. Dadurch könnten Angreifende SAP-ERP-Systeme manipulieren. Dann könnten vertrauliche Daten abfließen, Dienste ausfallen oder ganze Geschäftsprozesse stillstehen.

2.3. Mangelnde Planung, Umsetzung und Dokumentation eines SAP-Berechtigungskonzeptes

SAP-Berechtigungskonzepte sind fachlich und technisch komplex. Aufgrund dieser hohen Anforderungen werden sie in vielen Institutionen kaum oder nur ungenügend geplant und umgesetzt. Fehlt jedoch ein durchdachtes Berechtigungskonzept, werden z. B. Konten oft mehr Berechtigungen als notwendig zugewiesen. Diese Konten könnten dann das SAP-ERP-System vorsätzlich manipulieren oder versehentlich beschädigen. Somit ist die Integrität, Vertraulichkeit und Verfügbarkeit gefährdet.

Darüber hinaus muss das Design der Berechtigungen in S/4HANA-Systemen zwischen den integrierten Komponenten ABAP, HANA und NetWeaver Gateway (für Fiori-Anwendungen) genau abgestimmt und synchronisiert werden, da ansonsten widersprüchliche Berechtigungen vergeben werden könnten.

Wird das SAP-Berechtigungskonzept nicht ausreichend dokumentiert, können vergebene Berechtigungen nicht mehr nachvollzogen und somit gepflegt werden. So ist es z. B. möglich, dass bereits ausgeschiedene oder mit neuen Aufgaben betraute Mitarbeitende immer noch auf SAP-ERP-Systeme zugreifen können.

2.4. Fehlende SAP-Dokumentation und fehlende Notfallkonzepte

Gibt es keine Dokumentation für das SAP-ERP-System oder wird diese nicht gepflegt, lässt sich nicht mehr nachvollziehen, wie das SAP-ERP-System mit welchen Einstellungen aufgebaut wurde. Dadurch verzögern sich z. B. im Notfall die Wiederanlaufzeiten und geschäftskritische Prozesse fallen eventuell komplett aus. Diese Gefahr besteht auch, wenn es keine Notfallpläne gibt, die detailliert beschreiben, wie die Verantwortlichen im Ernstfall vorgehen sollen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.2 *SAP-ERP-System* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachabteilung, Notfallbeauftragte, Entwickelnde

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.